

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité d'Internet Explorer

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2004-ALE-012>

Gestion du document

Référence	CERTA-2004-ALE-012-002
Titre	Vulnérabilité d'Internet Explorer
Date de la première version	09 novembre 2004
Date de la dernière version	02 décembre 2004
Source(s)	Bulletin de sécurité Microsoft MS04-040 Bulletin de sécurité CERTA-2004-AVI-383 Bulletin de vulnérabilité VU#842160 Bulletin d'alerte AusCERT AL-2004.038
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire à distance.

2 Systèmes affectés

Internet Explorer 6 est vulnérable sous les différentes versions de Microsoft Windows.

Selon les vérifications effectuées par les différents CERTs mondiaux sur plusieurs configurations :

- Internet Explorer 6 sous Microsoft Windows XP Service Pack 1 est vulnérable ;
- Internet Explorer 6 sous Microsoft Windows 2000 est vulnérable ;
- Internet Explorer 6 sous Microsoft Windows XP Service Pack 2 semble ne pas être vulnérable au programme d'exploitation « *Proof of concept* » actuel. Cependant, il se pourrait qu'une future version de ce programme affecte ce type de configuration.

Certaines application telles que Outlook, Outlook Express, AOL, Lotus Notes qui utilisent le contrôle ActiveX du navigateur Internet Explorer 6 pourraient être également affectées par cette vulnérabilité.

3 Résumé

Une vulnérabilité découverte dans Internet Explorer permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système vulnérable.

4 Description

Le logiciel de navigation Internet Explorer 6 de Microsoft présente une vulnérabilité de type débordement de mémoire (*Buffer Overflow*) due à un mauvais traitement des attributs SRC et NAME des balises <FRAME> et <IFRAME> qui permettent aux développeurs d'insérer des cadres dans une page HTML. Cette vulnérabilité permet à une personne mal intentionnée d'exécuter du code arbitraire, avec les privilèges de la victime, à l'aide d'une page HTML ou d'un courrier électronique malicieusement constitués.

Un programme de démonstration (« *Proof of concept* ») exploitant cette vulnérabilité d'Internet Explorer 6 est d'ores et déjà diffusé sur l'Internet. Cette preuve de faisabilité concerne différentes versions du système d'exploitation Windows.

Plusieurs éditeurs d'anti-virus ont également recensé la diffusion d'un ver (*le nom du virus diffère selon les éditeurs*) exploitant cette vulnérabilité.

5 Contournement provisoire

Contournement provisoire pour Microsoft Windows :

- désactiver `Active Scripting` et `ActiveX` dans les paramètres de sécurité d'Internet Explorer (cf. Documentation). L'opération qui consiste à désactiver l'`Active Scripting` et l'`ActiveX` permet de rendre inefficace l'actuel programme d'exploitation « *Proof of concept* ». Il n'est pas exclu que la vulnérabilité reste exploitable, même si tous les scripts sont désactivés. ;
- utiliser un autre logiciel de navigation.

Pour Microsoft Windows XP uniquement :

- appliquer le `Service Pack 2` pour Windows XP protège du « *Proof of concept* ». Cependant le `Service Pack 2` pour Windows XP introduit quelques nouveaux mécanismes de sécurité. Toutes les applications n'ont pas été conçues pour tenir compte de ces mécanismes. Le fonctionnement de ces applications peut être altéré dans des proportions plus ou moins grandes. Il est donc préférable de tester avant de déployer à grande échelle.

6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. Documentation).

7 Documentation

- Bulletin de sécurité Microsoft MS04-040 :
<http://www.microsoft.com/technet/security/bulletin/MS04-040.mspx>
- Bulletin de sécurité CERTA-2004-AVI-383 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-383/index.html>
- Bulletin d'alerte US-CERT VU#842160 :
<http://www.kb.cert.org/vuls/id/842160>
- Bulletin d'alerte AusCERT AL-2004.038 :
<http://www.auscert.org.au/render.html?it=4527>
- Comment désactiver les contenus actifs sous Internet Explorer :
<http://support.microsoft.com/default.aspx?scid=kb;en-us;q154036>
- Comment activer `My Computer Security Zone` dans les options Internet :
<http://support.microsoft.com/?kbid=315933>
- Some programs seem to stop working after you install Windows XP Service Pack 2
<http://support.microsoft.com/default.aspx?kbid=842242>

Gestion détaillée du document

09 novembre 2004 version initiale.

10 novembre 2004 Correction des liens dans la section Documentation.

02 décembre 2004 Ajout de la section *Solution* et des références aux mises à jour de sécurité Microsoft.